Research Paper | Engineering | E-ISSN No : 2454-9916 | Volume : 7 | Issue : 10 | Oct 2021

ANOMALY DETECTION IN COMPLEX NETWORK USING COMMUNITY DETECTION CONCEPT

*Azadeh Oliyaei[1] | Dr Alireza Aliahmadi[2]

[1]Department of Industrial Engineering, PhD Candidate, Iran University of Science and Technology, Tehran, Iran. (*Corresponded Autor)

[2]Department of Industrial Engineering, Faculty of Engineering, Iran University of Science and Technology, Tehran, Iran

ABSTRACT

Discovering anomalous users in the social network is a crucial problem in analyzing network. The previous works focus on a network with just one type of interaction among the entities. However, the relationship among people is highly complex, and users have multiple types of interaction in a social network. On the other hand, users tend to form a community in the social network such that normal users usually have friends who are frends themselves, and anomalous users typically do not follow this rule. In this paper, we consider the detection of anomalous nodes in the multi-layer social network by combing the information in each layer of the network. We propose a pioneering algorithm based on the community detection method and assign the anomaly score to each user and rank them. Experimental result on real dataset shows that the proposed algorithm can recognize anomalous users in the multi-layer social network.

KEYWORDS: Anomaly Detection, Social Network, Anomalous Users, Community Detection.

INTRODUCTION:

Nowadays, many complex systems are modeled by the network. Arab et al., (2014) and Aqib et al., (2018) utters that network is sets of nodes, representing entities, connected by edges, representing the relationship between entities based. For example, a social network can be modeled as a graph where nodes represent users; and the edges are the relationship between users based on the definition of Diesner et al., (2005). A network that is modeled one type of relation is called a single layer network and multi types of relations among entities are viewed as a multi-layer network. Most complex systems are modeled as a multi-layer network. Network analysis is a powerful tool for analyzing data in many aspects, including detecting community Chunaev, P (2020), find influential nodes Debnath et al., (2020), and recognize abnormal behavior in the network Song et al., (2019). In this research, we propose the algorithm to detect anomalous nodes in the multi-layer network.

The anomaly detection is a difficult task due to there is not any unique definition of the anomaly, and also it depends on the application and problem on hand according to Bindu et al., (2017). Chandola et al., (2009) mention that an anomaly is an entity that behaves differently from other entities. The traditional definition of anomaly is entity that deviates a lot from other entities by Hawkins (1980). Anomaly is an observation that is inconsistent with other observations based on the definition of Nanavati et al., (2008). Detecting anomaly is highly crucial because it causes damage to the system. For instance, anomaly represents fraudulent and illegal behavior in the social network that can harm to other users.

Anomaly detection in the network is different from anomaly detection technique in non-network data because of analyzing the interaction among entities. Hence, it is a crucial problem, and researchers pay attention to it in recent years. Most of the works have been proposed to solve anomaly detection on a single layer network; however, most of the real systems are modeled as a multi-layer network according to Kivel (2014)- Kunpeng et al (2020). Most anomaly detection algorithms on a multi-layer network convert a network into a single layer network and applied anomaly detection algorithms that are developed for a single layer. Aggregation multi-layer network into a single layer causes losing hidden information on the network. Therefore, developing an algorithm to detect anomaly in the multi-layer network is an essential and ongoing research area. In this research, the algorithm purpose of identifying the anomalous node in the multi-layer network.

The proposed algorithm finds the anomalous node in the multi-layer network by using a community detection concept. The algorithm uses the structure of the node's egonent and super-egonent in order to compute the community of each node in the network. Egonent is a one-step neighborhood of node including all its neighbors and interactions and its node. Also, super-egonent is one and two-step neighborhood. Then, the algorithm is calculated anomaly score based on community detection of each node of the network. After that, the final anomaly score of each node is a linear combination of anomaly scores of a node in different layers. In this algorithm, the node contribution concept is introduced as a linear coefficient. Node contribution shows that the degree of the node's importance in each layer. Finally, the anomaly score is ranked to recognize anomalous nodes in the network. The proposed algorithm applies to six datasets, and the results show that it recognizes anomalous nodes effectively. The organization of the paper is as follows. Section 2 discusses the previous research on anomaly detection. In section 3, the problem and algorithm are expressed. Experimental analysis and results are presented in section 4. Finally, the paper concludes in section 5.

RELATED WORKS:

Most of the research in this area work on anomaly detection techniques on non-network data. The surveys have been provided on anomaly detection on non-network data, including Savage et al., (2016). In one of the overview of general anomaly detection which proposed by Chandola et al., (2009) develops previous works of anomaly detection techniques into six classes, classification, clustering, nearest neighbor, statistical, information-theoretic, and spectral analysis. Anomaly detection on network data is introduced in the workshop was held at ACM 2013 by Akoglu et al., (2010). In the networked data, anomaly detection has been researched very well Akoglu et al., (2010), Chandola et al., (2012), Gao et al., (2010), Hassanzadeh et al., (2012), Hassanzadeh et al., (2013a), Hassanzadeh et al., (2013b), Muller et al., (2013), Sun et al., (2010), Sun et al., (2005), Tong et al., (2011), Xu et al., (2007), Yang et al., (2015), Aggarwal et al., (2011), Ji et al., (2013), and Miller et al., (2015). The recent survey on anomaly detection techniques in the social network data is presented Bindu et al., (2016). These works can be divided into two classes, behavior-based, structure-based according to Hassanzadeh et al., (2012). Behavior-based considers users' behavior and structure-based mines users' usage patterns based on Hassanzadeh et al., (2012). Also, Zoppi et al (2020) proposed a multi-layer anomaly detection framework for complex dynamic system. A comprehensive novel model for network speech anomaly detection system using deep learning approach put forward by Manimaran et al (2020). Some application researches in the area including Ullah et al., (2020), Lia et al., (2019) and Zhang et al., (2019).

However, most of the works consider one type of interaction on the network and apply anomaly detection. Also, most techniques, tools, and algorithms can apply on a single layer network, and we cannot directly use the multi-layer network, and it is necessary to combine a multi-layer network into a single layer. The result of that loses hidden information on the network. There is a limit work on anomaly detection on multi-layer. To the best of our research, there is one research which addresses on Bindu et al., (2017). This work uses the network structure based in order to detect anomalous nodes in the multi-layer network. So, it is highly essential to develop anomaly detection on the multi-layer network. In this work, we propose the algorithm to detect anomalous nodes in the multi-layer network.

The Proposed Algorithm:

In this section, we propose a new algorithm in order to detect anomalous nodes in the multi-layer network. Most of the previous researches focus on a single layer network. However, the real networks have multi types of interactions, and they cannot model as a single layer without losing useful information. On the other hand, anomaly detection in a complex network is a difficult problem because there is no universal definition of the anomaly and wholly related to the problem at hand. So, developing an algorithm or a tool is a highly important and also ongoing area for research.

In this work, we address the algorithm to capable of detecting anomalous nodes in the multi-layer network, which includes three phases, computing community, computing anomaly score, an anomaly score ranking. In the following section, we put forward the definition of the problem, and then we discuss all phases of the algorithm in detail.

Problem Definition:
The problem is defined as follows. Suppose multi-layer network $G=\{G_1.G^2.....G_l\}$ with a L network layers, each layer represents one type of interaction and it considers as a single layer network $[G_l=(V_1.E_1)]$. Every node can exist in more than one layer and every single network has its adjacency matrix that can be defined $A_G=\{A_1,A_2,...,A_n\}$ where $A_l=\{1\}$ if only if i and j are connected in layer l. The purpose of this research is to develop an algorithm in order to detect anomalous nodes in the multi-layer network.

SOLUTION METHODOLOGY:
In this section, we address our algorithm in detail. Our algorithm calculates the community of each node in individual layers. Then, the anomaly score assigns to all nodes of the network according to the community of nodes. The anomaly score of the corresponding nodes from each layer is then combined based upon the node contribution in each layer in order to calculate total anomaly scores of a node in the multi-layer network. Finally, the nodes of the multi-layer network are ranked based on anomaly scores.

As there is not any interdependency among the operations on individual layers of the network, we compute the community on different layers in a parallel.

Phase 1- Compute Community:
Entities of the most real system tend to form communities based on their similarity and interest. Therefore, the information from communities' structure can be useful for analyzing entities' behavior in order to detect anomalous node. In this work, the anomaly score assigns to each node of the network in every layer based on community detection. For this purpose, the following steps are taken.

1. Generate Super-egonent of each node in every layer of network. For instance, node i: $egonent_i=\{i,i_1,i_2,...,i_n\}$
   $Super\text{-}egonent_i=\{egonent_i,\text{egonent}(i_2),\ldots,egonent(i_n)\}$

2. Based on Infomap community detection algorithm [], the community assign to each node of its super-egonent. For example, the community is assigned to every node which exists in *Super-egonent$_i$*.

3. For each node in every layer of the network, its neighbor's is selected.

4. Two anomaly score assigned to each node in every layer based on the diversity of the he neighbor's community and similarity of node community with its neighbors' community which demonstrate with SF_i^C and SS_i^C respectively.

   If all neighbors of node i belong to the same community or the node i dose not have any neighbors, the SF_i^C of the node i is equal to zero and SF_i^C of node i become more if the variety of neighborhood of community is high. So, the SF_i^C s calculated as follow:

$$SF_i^C = \begin{cases} 0 & \textit{all neighbors have same community or no neighbors} \\ \frac{\textit{Number of different communities}}{\textit{Total node in Eqonent}-1} & o.w \end{cases}$$

   SS_i^C is calculated based on the similarity of the community of node i with its neighbors' communities. If the node i does not have any neighbors, the SS_i^C of the node i is equal to zero. So, the SS_i^C is calculated as follow:

$$SS_i^C = \begin{cases} 0 & \textit{no neighbors} \\ 1-\frac{\textit{number of neighbors with same community of node i}}{\textit{Total node in Eqonent}-1} & o.w \end{cases}$$

5. Finally, two anomaly scores combine by the following equation.

$$S_i^C = \alpha_1 SF_i^C + \alpha_2 SS_i^C$$

Where $\alpha_1 = \alpha_2 = \frac{1}{2}$

Phase 2- Compute Anomaly Score:
After computing anomaly score based on community, the final anomaly score of each node is calculated as linear combinations of anomaly scores in the each single network. Since each relationship may have different significance in the real world, assigning different degrees to each node in different layers of the network is more reliable. So, node contribution is defined in order to calculate the importance of each node in the individual layer. Node contribution demonstrates how a specific node and its neighbors are connected to each other and consider as the coefficient of linear combinations. Providing that the connectivity of the node is dense in the specific layer, the node contribution is high in comparison of this node in other layers which the connectivity of the node is sparse. More formally, the node contribution for each layer is defined as:

$$NC_i^l = \frac{d_i^l}{\sum_{l=1}^{L} d_i^l}$$

Where is d_i^l the degree of node i in layer l^th.

Final anomaly score of each node is defined as follow.

$$AnomalyScore_i = \sum_{l=1}^{l} NC_i^l \times S_i^C$$

Phase 3- Ranking Anomaly Score:
In the previous phases, the anomaly score is computed for each node. After the calculation of nodes' anomaly score, the nodes are ranked based upon their anomaly score. In other words, the nodes are sorted based upon their degree of deviation from the normal.

EXPERIMENTAL ANALYSIS AND DISCUSSION:

The effectiveness and efficiency of our algorithm is examined by six real multi-layer networks. We implement the algorithm on an Intel Core I5 CPU@ 2.60 GHz machine with 6 GB RAM running on window 8 operation system. The algorithm is implemented in R programming language and using igraph library. As there is no correlation among the operations in a different layer, we implement all phases of our algorithm in parallel. First, the six datasets are introduced and then the result of our algorithm on these datasets is discussed.

1. **Noordin Top Terrorist Network:** The Noordin Top Terrorist Network which proposed by Roberts et al., (2011) is a four layer multi-layer network of Indonesian terrorists. The dataset includes information of 78 terrorists about their operation, communications, trust, and financial, among them.

2. **Social Evolution Dataset:** The Social Evolution Dataset which proposed by Madan et al., (2012) is a five layer multi-layer network of student of MIT dormitory. The dataset includes information of student relationships such as close friend, socialize twice per week, political discussant, Facebook all tagged photos, and blog live journal Twitter.

3. **Aarhus:** The Aarhus which proposed by Magnani et al., (2013) is a five layer multi-layer network of social interactions of research department of Aarhus University. The dataset includes information about lunch, co-authorship, Facebook, work, and leisure.

4. **DBLP_C:** The DBLP_C which proposed by Berlingerio et al., (2013) is a six layer multi-layer network of co-authorship on the computer science conference. Each layer of this network is related to a specific conference. The node of network is an author, and two author are connected to each other if they have paper together. The dataset includes information about VLDB, SIGMOD, CIKM, SIGKDD, ICDM, and SDM.

5. **ArXiv:** The arXiv which proposed by De Domenico et al., (2015) is a 13 layer multi-layer network of co-authorship network of the free scientific repository arXiv. The dataset includes information about physics.soc-ph.data-an, physics, physics.bio-ph, math.OC, math-ph, cond-mat.stat-mech, cond-mat.dis-nn, q-bio, nlin.AO, q-bio.BM, cs.SI, cs.CV.

6. **GTD:** The Global Terrorism Database (GDT) which proposed by Berlingerio et al., (2011) is a 124 layer multi-layer network of terrorist attack incidents in the world. The nodes of this network are terrorist organizations and they are connected to each other if they have attacked the same country in the same year. Also, each layer represents one country. We use all terrorist attacks occurred during the year 1970-2008.

The summary of each dataset is presented on table

Dataset	Nodes	Edges	Layers
Noordin Top	78	911	4
Social Evolution	84	31,918	5
Aarhus	61	620	5
DBLP	6,771	19,345	6
arXiv	14,065	59,026	13
GTD	2,509	32,279	124

RESULTS AND DISCUSSION:

The validation of anomaly detection algorithms is not simple because there is no labeled dataset [22, 67], and there is no standard method for the validation of anomaly detection algorithms [5, 14]. However, we evaluate the result of our algorithm on six real multi-layer networks.

Moreover, most of the work in the anomaly detection of network data conduct in a single layer network and researchers convert a multi-layer network into a single layer in order to apply developed algorithms for the single layer. In this work, we aggregate all information that exists in different layers to get a single-layer network in order to apply the traditional network analysis algorithms. The aggregated network is called the aggregation algorithm. The nodes of the aggregation network are all nodes in the multi-layer network, and edges are all edges in the multi-layer network. Also, implement the proposed algorithm in the aggregation network.

We compare our results with the aggregation algorithm. Top ten ranked nodes recognized by our algorithm, and the aggregation algorithm are shown in the following table. Since there is no labeled data with ground truths, the top anomalous nodes are manually considered in order to whether they are anomalous or not in the Noordin Top data node 57 is a top anomalous node in the Noordin dataset which indicates Mohamed, the head of the terrorist group. All results demonstrate that in the table –

Dataset	Rank	Our Algorithm	Aggregation Algorithm
		Node	Node
Noordin Top	1	57	57
	2	21	21
	3	70	71
	4	63	23
	5	67	66
	6	43	44
	7	68	68
	8	4	4
	9	51	51
	10	72	50
Social Evolution	1	15	13
	2	52	41
	3	12	8
	4	11	33
	5	32	75
	6	49	7
	7	67	58
	8	19	17
	9	53	56
	10	993	2495

	10	74	82
Aarhus	1	7	7
	2	22	1
	3	10	60
	4	23	22
	5	53	34
	6	44	44
	7	36	26
	8	20	53
	9	8	23
	10	50	61
DBLP_C	1	6815	558
	2	558	4131
	3	720	720
	4	6187	534
	5	4181	1358
	6	7559	6818
	7	6810	14234
	8	6178	3525
	9	3525	16216
	10	6813	233
ArXiv	1	125	479
	2	127	83
	3	8156	218
	4	468	172
	5	10463	54
	6	10464	715
	7	3680	578
	8	10936	80
	9	10939	1751
	10	480	842
GTD	1	406	81
	2	253	161
	3	241	134
	4	372	1460
	5	1998	2245
	6	2057	109
	7	1784	571
	8	952	836
	9	299	203

CONCLUSION:

Detecting anomalous nodes in the multi-layer social network is a serious problem. Even though various techniques and algorithms have been proposed for single layer network, there is limit work on the multi-layer network it is an unexplored area of research.

In this research, we proposed the algorithm based on community detection method in order to detect anomalous node in the multi-layer network. Since, people tend to form community in the social network, so the normal user have the same community as its friends. The neighborhood of anomalous nodes have different community. We use this concept to detect anomalous node in the network data. We assign the anomaly score to each node in different layer based on the community of their neighborhood after that we combine different anomaly score of specific node in different layer with each other based on node contribution. After that, the anomaly score of each node is ranked.

There is no standard technique to evaluate the algorithm and our algorithm is the pioneer algorithm in this area. So we validate our algorithm in the six real dataset and evaluate manually the result.

REFERENCES:

I. Aggarwal, CC., Zhao, Y., and Philip, SY. (2011) ' Outlier detection in graph streams', 2011 IEEE 27th International Conference on Data Engineering, pp. 399–409.

II. Aqib Javad, M., Younis , MH., Latif, S., Qadir, J., and Baig, A. (2018) ' Community detection in networks: A multidisciplinary review', Journal of Network and Computer Applications, pp. 87–111.

III. Akoglu, L., Glohon, M., and Faloutsos, C. (2010) ' Oddball: Spotting anomalies in weighted graphs' Pacific-Asia Conference on Knowledge Discovery and Data Mining, pp. 410–421.

IV. Arab, M and Afsharchi, M. (2014) 'Community detection in social networks using hybrid merging of sub-communities', Journal of Network and Computer Applications, pp. 73-84

V. "Berlingerio, M., Coscia, M., Giannotti, F., Monreale, A., and Pedreschi, D., (2013a) 'Multidimensional networks: foundations of structural analysis' World Wide Web, pp. 567–593"

VI. Berlingerio, M., Coscia, M., and Giannotti, F., (2011b) 'Finding and characterizing communities in multidimensional networks' Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on, IEEE, pp. 490–494.

VII. Bindu, P.V., Thilagam, S., and Ahuja, D., (2017) ' Discovering suspicious behavior in multilayer social networks' Computers in Human Behavior, pp. 568-582.

VIII. Bindu, P.V., and Thilagam, S., (2016) ' Discovering suspicious behavior in multilayer social networks' Journal of Network and Computer Applications, pp. 213-229.

IX. Chandola, V., Banerjee, A., and Kumar, V., (2009) 'Anomaly detection: A survey' ACM Computing Surveys (CSUR), pp. 41-15.

X. Chandola, V., Banerjee, A., and Kumar, V., (2012) 'Anomaly detection for discrete sequences: A survey' Knowledge and Data Engineering, IEEE Transactions on Knowledge and Data Engineering, pp.823–839.

XI. Chunaev, P., (2020) 'Community detection in node-attributed social networks: A survey' Computer Science Review.

XII. Savage, D., Zhang, X., Yu, X., Chou, P., and Wang, Q., (2014) 'Anomaly Detection in Online Social Networks' Social Networks, pp. 62-70.

XIII. Debnath, S., Sarkar, D., and Jana, P., (2020).' Top-k Influential Nodes Identification Based on Activity Behaviors in Egocentric Online Social Networks'. Computational Intelligence in Pattern Recognition, pp. 463-475.

XIV. De Domenico, M., Lancichinetti, A., Arenas, A., and Rosvall, M., (2015) ' Identifying modular flows on multilayer networks reveals highly overlapping organization in interconnected systems' Phys. Rev.

XV. Diesner, J., Frantz, T.L., and Carley, K.M. (2005) 'Communication networks from the Enron email corpus “It's always about the people. Enron is no different', Computational & Mathematical Organization Theory.

XVI. Gao, J., Liang, F., Fan, W., Wang, C., Sun, Y., and Han, J., (2010) 'On community outliers and their efficient detection in information networks', in: Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining, ACM. pp. 813–822.

XVII. Hassanzadeh, R., Nayak, R., and Stebila, D., (2012) 'Analyzing the activeness of Graph Metrics for Anomaly Detection in Online Social Networks' International Conference on Web Information Systems Engineering, pp. 624–630.

XVIII. Hassanzadeh, R., and Nayak, R., (2013a) 'A rule-based hybrid method for anomaly detection in online-social-network graphs' 25th International Conference on, IEEE. pp. 351–357.

XIX. Hassanzadeh, R., and Nayak, R., (2013b) 'A semi-supervised graph-based algorithm for detecting outliers in online-social-networks' Proceedings of the 28th Annual ACM Symposium on Applied Computing, ACM. pp. 577-582.

XX. Hawkins, D.M., (1980) 'Identification of outliers.

XXI. Ji, T., Yang, D., and Gao, J., (2013) 'Incremental local evolutionary outlier detection for dynamic social networks' Proceedings, Part II, of the European Conferenceon Machin Learning and Knowledge Discovery in Databases, pp. 1–15.

XXII. Kunpeng, Z., Liang, Z., Zijian, L., and Ning, J., (2020) ' A deep learning based multitask model for network-wide traffic speed prediction' Neurocomputing, pp. 438–450.

XXIII. Kivel¨a, M., Arenas, A., Barthelemy, M., Gleeson, J.P., Moreno, Y., and Porter, M.A., (2014) 'Multilayer networks'.

XXIV. Lia, Y., Zhou, K., Lin, S., and Lo, N., (2019) ' F1ow-based Anomaly Detection Using Multilayer Perceptron in Software Defined Networks' IEEE Pervasive Computing, pp. 36–45.

XXV. Madan, A., Cebrian, M., Moturu, S., Farrahi, K., and Pentland, A., (2012) 'Sensing the” health state” of a community' IEEE Pervasive Computing, pp. 36–45.

XXVI. Manimaran, A., Chandramohan, D., Shrinivas. S.G., and Arulkumar, N., (2020) 'A comprehensive novel model for network speech anomaly detection system using deep learning approach ' International Journal of Speech Technology, pp. 305-313.

XXVII. Miller,B.A., Arcolano,N., and Bliss,N.T., (2013) 'Efficient anomaly detection in dynamic, attributed graphs: Emerging phenomena and big data' Intelligence and Security Informatics (ISI), 2013 IEEE International Conference on, IEEE. pp. 179–184.

XXVIII. Miller,B.A., Arcolano,N., and Bliss,N.T., (2013) 'Efficient anomaly detection in dynamic, attributed graphs: Emerging phenomena and big data' Intelligence and Security Informatics (ISI), 2013 IEEE International Conference on, IEEE. pp. 179–184.

XXIX. Muller, E., S´anchez, P.I., Mulle, Y., and Bohm, K., (2013) 'Ranking outlier nodesin subspaces of attributed graphs' Data Engineering Workshops (ICDEW), 2013 IEEE 29th International Conference on, IEEE. pp. 216–222.

XXX. Nanavati, A.A., Gurumurthy, S., Das, G., Chakraborty, D., Dasgupta, K., Mukherjea, S., and Joshi, A., (2006) 'On the structural properties of massive telecom call graphs: findings and implications' Proceedings of the 15th ACM international conference on Information and knowledge management. ACM, pp. 435–444.

XXXI. Roberts, N., Everton, S.F., (2011) 'Roberts and everton terrorist data: Noordin top terrorist network (subset)'.

XXXII. Savage, D., Zhang, X., Yu, X., Chou, P., and Wang, Q., (2014) 'Anomaly Detection in Online Social Networks' Social Networks, pp. 62-70.

XXXIII. Song, C., Liu, W., Liu, Z ., and Liu, X., (2019) ' User abnormal behavior recommendation via multilayer network'.

XXXIV. Sun, H., Huang, J., Han, J., Deng, H., Zhao, P., and Feng, B., (2010) 'gskeletonclu: Density-based network clustering via structure-connected tree division or agglomeration' Data Mining (ICDM) ,2010 IEEE10th International Conference on, IEEE, pp. 481–490.

XXXV. Sun, J., Qu, H., Chakrabarti, D., and Faloutsos, C., (2005) 'Neighborhood formation and anomaly detection in bipartite graphs' Data Mining, Fifth IEEE International Conference on, IEEE.

XXXVI. Ullah, W., Ullah, A., Haq, L., Muhammad, K., Sajjad M., and Baik, S., (2020) 'CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks'.

XXXVII. Tong, H., and Lin, C.Y., (2011) 'Non-Negative Residual Matrix Factorization with Application to Graph Anomaly Detection' SDM. SIAM, pp. 143–153.

XXXVIII. Xu, X., Yuruk, N., Feng, Z., and Schweiger, T.A., (2007) 'Scan: a structural clustering algorithm for networks' Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, ACM, pp. 824–833.

XXXIX. Yang, W., Shen, G.W., Wang, W., Gong, L.Y., Yu, M., and Dong, G.Z., (2015) 'Anomaly detection in microblogging via co-clustering' Journal of Computer Science and Technology, pp.1097–1108.

XL. Zhang, S., Xiao, K., Carranaz, E., Yang, F., and Zhoa, Z., (2019) Integration of auto-encoder network with density-based spatial clustering for geochemical anomaly detection for mineral exploration'. Computers & Geosciences, pp.43-56.

XLI. Zoppi, T., Ceccarelli., and Bondavalli, A., (2020) 'MADneSs: a Multi-layer Anomaly Detection Framework for Complex Dynamic Systems'. IEEE Transactions.